IN THE CLAIMS

What is claimed is:

1. A method for transferring files, comprising:

receiving a request to transfer a file;

locating the requested file stored in a memory;

computing a unique identifier corresponding to the requested file;

choosing a first key, K_1;

encrypting the first key, K_1, and the unique identifier with a second key, K_2, to generate a first value;

encrypting the requested file with the first key, K_1, to generate a second value; and

transferring the first and second values.

2. The method of claim 1, wherein the requested file is an encrypted file.

3. The method of claim 1, further comprising transferring the first key, K_1, upon a payment being made.

4. The method of claim 3, further comprising decrypting the second value with the first key, K_1, to generate the requested file.

5. The method of claim 1, further comprising interrupting the transmission of the second value.

6. The method of claim 5, further comprising continuing the transmission of the second value without retransferring the entire second value.

7. The method of claim 1, wherein the second key, K2, is a public key having a corresponding private third key, K3.

8. The method of claim 1, wherein the unique identifier is an MD5 checksum of the requested file.

9. The method of claim 1, wherein the unique identifier corresponds to binary information.

10. The method of claim 1, wherein the unique identifier corresponds to ASCII information.

11. A method for transferring files, comprising;

receiving a request to continue downloading a partially transferred encrypted file;

receiving a first value corresponding to an encrypted quantity wherein the quantity comprises a first key, K_1, and a first unique identifier corresponding to unencrypted form of the encrypted file;

recovering the first key, K_1, and the first unique identifier using a second key, K_2;

locating an unencrypted form of the encrypted file based on the first unique identifier;

computing a second unique identifier from the unencrypted form of the encrypted file;

confirming that the first and second unique identifiers are equal;

encrypting the unencrypted form of the encrypted file with the first key, K_1, to generate the requested encrypted file; and

transferring a remaining portion of the partially transferred encrypted file.

12. The method of claim 11, further comprising appending the transferred remaining portion with the partially transferred file.

13. The method of claim 12, further comprising transferring the first key, K_1, upon a payment being made.

14. The method of claim 13, further comprising decrypting the appended file with the first key, K1.

15. The method of claim 11, further comprising interrupting the transmission of the remaining portion of the partially transferred encrypted file.

16. The method of claim 15, further comprising continuing the transmission of the remaining portion of the partially transferred encrypted file.

17. The method of claim 11, wherein the second key, K_2, is a public key having a corresponding private third key, K_3.

18. The method of claim 11, wherein the first and second unique identifiers are MD5 checksums.

19. The method of claim 11, wherein the unique identifier corresponds to binary information.

20. The method of claim 11, wherein the unique identifier corresponds to ASCII information.

21. A method for verifying downloaded files, comprising;
receiving a first unique identifier corresponding to a downloaded encrypted file, wherein the encrypted file was computed using a first key, K_1;
receiving a first encrypted value computed using a second key, K_2, wherein the encrypted value contains information relating to a second unique identifier and the first key, K_1;
extracting the second unique identifier and the first key, K_1, using a third key, K_3;
retrieving a third unique identifier corresponding to a verified file having the second unique identifier;
confirming that the first and third unique identifiers are equal; and
transferring the first key, K_1.

22. The method of claim 21, wherein the first, second, and third unique identifiers are MD5 checksums.

23. The method of claim 21, wherein the second key, K2, is a public key and the third key is a private key.

24. The method of claim 21, wherein the first, second, and third unique identifiers corresponds to binary information.

25. The method of claim 21, wherein the unique identifier corresponds to ASCII information.

26. The method of claim 21, further comprising decrypting the downloaded encrypted file using the first key, K_1.

27. The method of claim 21, further comprising locating an unencrypted form of the encrypted file based on the second unique identifier, computing an encryption of the located unencrypted form of the encrypted file with the first key, K_1, and computing the third unique identifier from the computed encryption.

28. An apparatus for transferring binary files, comprising:
means for receiving a request to transfer a file;
means for locating the requested file stored in a memory;
means for computing a unique identifier corresponding to the requested file;
means for choosing a first key, K_1;
means for encrypting the first key, K_1, and the unique identifier with a second key, K_2, to generate a first value;
means for encrypting the requested file with the first key, K_1, to generate a second value; and
means for transferring the first and second values.

29. The apparatus of claim 28, wherein the requested file is an encrypted file.

30. The apparatus of claim 28, further comprising means for transferring the first key, K_1, upon a payment being made.

31. The apparatus of claim 30, further means for comprising decrypting the second value with the first key, K_1, to generate the requested file.

32. The apparatus of claim 28, further comprising means for interrupting the transmission of the second value.

33. The apparatus of claim 32, further comprising means for continuing the transmission of the second value without retransferring the entire second value.

34. The apparatus of claim 28, wherein the second key, K2, is a public key having a corresponding private third key, K3.

35. The apparatus of claim 28, wherein the unique identifier is an MD5 checksum of the requested file.

36. The apparatus of claim 28, wherein the unique identifier corresponds to binary information.

37. The apparatus of claim 28, wherein the unique identifier corresponds to ASCII information.

38. An apparatus for transferring binary files, comprising;

means for receiving a request to continue downloading a partially transferred encrypted file;

means for receiving a first value corresponding to an encrypted quantity wherein the quantity comprises a first key, K_1, and a first unique identifier corresponding to unencrypted form of the encrypted file;

means for recovering the first key, K_1, and the first unique identifier using a second key, K_2;

means for locating an unencrypted form of the encrypted file based on the first unique identifier;

means for computing a second unique identifier from the unencrypted form of the encrypted file;

means for confirming that the first and second unique identifiers are equal;

means for encrypting the unencrypted form of the encrypted file with the first key, K_1, to generate the requested encrypted file; and

means for transferring a remaining portion of the partially transferred encrypted file.

39. The apparatus of claim 38, further comprising means for appending the transferred remaining portion with the partially transferred file.

40. The apparatus of claim 39, further comprising means for transferring the first key, K_1, upon a payment being made.

41. The apparatus of claim 40, further comprising means for decrypting the appended file with the first key, K1.

42. The apparatus of claim 38, further comprising means for interrupting the transmission of the remaining portion of the partially transferred encrypted file.

43. The apparatus of claim 42, further comprising means for continuing the transmission of the remaining portion of the partially transferred encrypted file.

44. The apparatus of claim 38, wherein the second key, K_2, is a public key having a corresponding private third key, K_3.

45. The apparatus of claim 38, wherein the first and second unique identifiers are MD5 checksums.

46. The apparatus of claim 38, wherein the unique identifier corresponds to binary information.

47. The apparatus of claim 38, wherein the unique identifier corresponds to ASCII information.

48. An apparatus for transferring binary files, comprising;

means for receiving a first unique identifier corresponding to a downloaded encrypted file, wherein the encrypted file was computed using a first key, K_1;

means for receiving a first encrypted value computed using a second key, K_2, wherein the encrypted value contains information relating to a second unique identifier and the first key, K_1;

means for extracting the second unique identifier and the first key, K_1, using a third key, K_3;

means for retrieving a third unique identifier corresponding to a verified file having the second unique identifier;

means for confirming that the first and third unique identifiers are equal; and

means for transferring the first key, K_1.

49. The apparatus of claim 48, wherein the first, second, and third unique identifiers are MD5 checksums.

50. The apparatus of claim 48, wherein the second key, K2, is a public key and the third key is a private key.

51. The apparatus of claim 48, wherein the first, second, and third unique identifiers corresponds to binary information.

52. The apparatus of claim 48, wherein the unique identifier corresponds to ASCII information.

53. The apparatus of claim 48, further comprising means for decrypting the downloaded encrypted file using the first key, K_1.

54. The apparatus of claim 48, further comprising means for locating an unencrypted form of the encrypted file based on the second unique identifier, means for computing an encryption of

the located unencrypted form of the encrypted file with the first key, K_1, and means for computing the third unique identifier from the computed encryption.